Cyber Security

SOC(Security Operation Center) Duration: 35+ Hours

1. CCNA Concepts (10 hours)

2. Basic explanation on DNS and DHCP. (2 hours)

3. Basic explanation on firewall, DLP, Proxy, IDS and IPS. (3 hours)

4. Basic explanation on CIA and AAA. (30 Mins)

5. Explanation on Threat, Risk and Vulnerability. (30 Mins)

6. Basic explanation on Security assessment tools like Firewall, DLP, IPS, IDS, Antivirus, Proxy, Email security gateway. (4 hours)

7. Basic training on Phishing mail analysis. (2 hours)

8. Basic training on threat hunting. (2 hours)

9. Training on Log Monitoring analysis. (2 hours)

10. Training on SIEM (Security Information and Event Management) Tool - Log monitoring and analysis of logs through SIEM, SIEM architecture. (3 hours)

11. Training on SOC Process and day to day activities of SOC (1 hour)

12. Training on Types of malwares with examples (2 hours)

13. Training on different types of cyber attacks (2 hours)

14. Training on Incident response process (1 hour)

15. Training on Cyber Kill Chain (1 hour)

- Above mentioned are the timings for covering the concepts.
- For better understanding of the course training we can conduct some extracurricular activities like
- conducting quiz on day to day basis and on the concepts covered on the respective days,
- giving some assignments to conduct seminar on the concepts covered,
- Taking mock interviews for every week on the concepts covered these are some of the ideas which may help for each one attending the training to better understand the course and concepts.